AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Special Agent Brian Stewart, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 3600 Beech Tree Ln. Okemos, MI 48864, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Homeland Security Investigations and have been since December 6, 2009. I have received training in computer crimes to include computer network intrusion and dark web related crimes. In addition, I have been involved in numerous investigations regarding child pornography, immigration, terrorism and human rights related investigations.

3. This affidavit is intended to show only that there is sufficient probable cause to search the PREMISES for evidence of violations 18 U.S.C. § 1519 (destruction, alteration, or falsification of records). This affidavit is intended to set forth sufficient information to establish probable cause for the requested warrant. It does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. On May 9, 2019, Top Flite Financial (TFF) made a report to the Michigan State Police, Michigan Cyber Crime Center (MC3), regarding an unauthorized access/network intrusion to their computer network. TFF worked with their contracted information technology company, Providence Consulting, to determine who was gaining unauthorized access to their computer network. TFF determined that someone had unauthorized access to their network and was logging in from IP address 68.61.175.164. This unauthorized access occurred from approximately April 26, 2019 to May 13, 2019. Homeland Security Investigations (HSI) used a subpoena and received confirmation from Comcast that the IP address 68.61.175.164 was assigned to Jessie Yu of 3600 Beech Tree Ln. Okemos, MI 48864 (the PREMISES). Jessie Yu or Jie Yu is the wife of Baoli Yang. Yang was the information technology administrator that was terminated from TFF on April 26, 2019.

5. On May 22, 2019, a State Search Warrant was authorized by the 55th Judicial District Court, State of Michigan. During that search, agents seized multiple computers. Subsequent forensic analysis revealed that three of those computers were used to access TFF's computer system after Yang was terminated on April 26, 2019.

6. Based on this and other evidence, the grand jury returned an indictment, charging both Yang and Yu with Wire Fraud in violation of 18 U.S.C. § 1343 in Count 1 and Computer Intrusion Causing Damage in violation of 18 U.S.C. § 1030 in Count 2. (R.1: Indictment, WDMI Case No. 1:20-CR-103, PageID.1-5.) Of particular importance to this search warrant, the

indictment alleges that Defendants altered the code of a file named "neemsoft.dll." (R.1: Indictment, WDMI Case No. 1:20-CR-103, PageID.3.) During the review and analysis of evidence in this case, the altered neemsoft.dll file has been referred to as "Bad Program Code."

7. Trial in the case of Yang and Yu was scheduled to begin February 23, 2022. Two days before trial, Yang's counsel emailed the Government's counsel, stating Yang found two items in his basement at the PREMISES over the weekend that he wished to introduce at trial. The two items provided by Yang were a Maxell CD-R Disc (80min/700MB; serial #: 7106C18K1 10) and a SanDisk Cruzer Glide 16GB Thumb Drive (serial #:BL211257601W).

8. On February 23, 2022, the parties appeared for the scheduled trial. Yang, through his attorney, reaffirmed his intent to introduce the two digital storage devices during trial because, according to Yang's attorney, these two digital storage devices contained exculpatory evidence.

9. The information provided by Yang, through his attorney, was that the Maxell CD-R Disc (80min/700MB; serial #: 7106C18K1 10) was obtained by Yang on January 7, 2009, from his predecessor. Yang stated through his attorney that the SanDisk Cruzer Glide 16GB Thumb Drive (serial #:BL211257601W) was used by Yang to upload data to TFF's servers during a server migration.

10. During the hearing on February 23, 2022, the district court ordered Yang's counsel to provide the items to the Government, which happened during the hearing. The court then continued the trial to allow the Government time to inspect the evidence.

11. On February 24, 2022, Michigan State Police, Information Technology Specialist (ITS) Luke Thelen conducted a forensics analysis of the Maxell CD-R Disc (80min/700MB; serial #: 7106C18K1 10) and a SanDisk Cruzer Glide 16GB Thumb Drive (serial #:BL211257601W). ITS Thelen completed his forensic exam on March 3, 2022. In reviewing the CD-R Disc, ITS Thelen found 11 instances of the file named NeemSoft.dll, but none of those files contained what was previously identified as the altered or "Bad Program Code."

12. ITS Thelen forensically examined the SanDisk Cruzer Glide 16GB USB Drive (serial #:BL211257601W). Of the many files observed, three files were observed as having come with the USB Drive when purchased. These files had a creation date of 8/8/2017.

13. Two files observed on the SanDisk Cruzer Glide contained similar code to what has previously been identified as the altered or "Bad Program Code". One file, named "Neemsoft.dll" was found on the thumb drive at the following file path: \New\neemsoft\bin. This file had a creation date of 2/22/2022 19:04:28 hours and a modified date of 7/21/2005 10:32 hours. The creation date is the date the file was placed on the flash drive. The modified date is the date the file was previously created on a different device, not the thumb drive. The other file, named "Neemsoft.dll" was found on the thumb drive at the following file path: \New\neemsoft\obj\Release. This file had a creation date of 2/22/2022 19:04:29 hours and a modified date of 4/8/2010 9:13 hours. The modified date is the date the file was previously created on a different device, not the thumb drive. Both files had the same hash value of

4F618F1F78433E1A59DE508009448247, despite being created on the thumb drive one second apart and having modified dates five years apart.

14. Based on my training and experience, and the analysis performed on this flash drive, several facts indicate that the files contained on the flash drive have been manipulated to indicate a date and time that is different from the actual date and time the file was created and modified. First, based on my training and experience, when I observe two files with the same exact "hash value" or unique identifier, like the files above, I know the files are the same. The difference is that the two files above have different dates and times associated with the same file. This would indicate the files have been manipulated in some capacity. Second, both files have a creation date of 2/22/2022, indicating they were placed on the drive on February 22, 2022; but that was over two years after Yang was terminated by TFF and two days before the trial was scheduled to begin. It is also the day Yang's attorney claimed Yang found the drive in his basement. Third, the file with a modified date of 7/21/2005, indicating it was originally created in 2005, appears to have been altered because it contains Yang's username (byang). Yang did not work at TFF in 2005; instead, he was initially hired in 2009. In other words, a file that appears to have been created in 2005 should not contain Yang's username because he did not work for TFF at the time. Fourth, the company that hosted TFF's servers, Providence Consulting, informed me that TFF only conducted one server migration during Yang's employment, which occurred in October of 2010. The thumb drive provided by Yang included files placed by SanDisk on the thumb drive on 8/8/2017. This indicates that Yang could not have used the thumb drive to upload data to the TFF

server's during the migration in October of 2010, because the thumb drive wasn't sold until sometime after SanDisk placed those files on the hard drive, which was 8/8/2017.

15. I am also aware of publicly available software that can manipulate file date and time creation and modification dates, without changing the file. This manipulation is often referred to as "time stomping". To use this time altering software, a person must have possession of a computer with the software installed. I am also aware that a computer may contain information indicating the drives and devices that were attached to it, such as the SanDisk drive at issue. The computer could still contain evidence of manipulation software and what digital media storage devices had been used on a particular computer.

16. Any computer that the thumb drive was inserted into or any computer that had manipulative software installed on it would still contain evidence that would be useful to this investigation. It is expected the search warrant will uncover computers that contain registry type files or files that have information about settings, options, software/hardware and other computer related information. These computers will contain event logs indicating if the computer clock was manipulated, if manipulation software was used and what digital storage devices were plugged into the computer.

17. ITS Thelen examined the Maxell CD-R Disc (80min/700MB; serial #: 7106C18K1 10). This CD had the following inscription on the CD: "Top Flite Financial"; "Backup Jan 7, 2009"; "Zak". All the files on the CD had no file creation or accessed dates and times. ITS Thelen examined all eleven files on the CD that were named "Neemsoft.dll". Ten of the files had a

modified date of 07/21/2005 9:32 and one file that had a modified date of 07/21/2005 10:32. All the "Neemsoft.dll" files had similar code to what has previously been presented as the unaltered, or "Good Program Code". ITS Thelen conducted a keyword search for "byang" and the search resulted in one file that had no relation to any neemsoft.dll or neemsoft program code.

TECHNICAL TERMS

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

c. Digital Storage Device: A digital storage device is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

19. As described above and in Attachment B, this application seeks permission to search records that might be found on the PREMISES for evidence of violations of 18 U.S.C. § 1519, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, under Rule 41(e)(2)(B).

20. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.

Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United

States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and

have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely

reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to tamper with or fabricate evidence, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

22. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

24. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by

persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

25. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.